A novel random neural network based approach for intrusion detection systems

Qureshi, Ayyaz-Ul-Haq; Larijani, Hadi; Ahmad, Jawad; Mtetwa, Nhamoinesu

Published in:
2018 10th Computer Science and Electronic Engineering (CEEC)

DOI:
10.1109/CEEC.2018.8674228

Publication date:
2019

Document Version
Author accepted manuscript

A Novel Random Neural Network Based Approach for Intrusion Detection Systems

Ayyaz-Ul-Haq Qureshi* Hadi Larijani*, Jawad Ahmad *, Nhamoinesu Mtetwa *,
* School of Engineering and Built Environment, Glasgow Caledonian University, Glasgow, United Kingdom.

***Abstract*—Computer security and privacy of user specific data is a prime concern in day to day communication. The mass use of internet connected systems has given rise to many vulnerabilities which includes attacks on smart devices. Regular occurrence of such events has made the availability of scalable Intrusion Detection System (IDS) a perilous challenge. An intelligent IDS should be able to stop the malicious activity before it destabilizes the core network and to achieve this goal we propose a novel Random Neural Network based Intrusion Detection System (RNN-IDS) in this paper. The performance is evaluated by training different numbers of input and hidden layer neurons with learning rates on benchmark NSL-KDD dataset for binary classification. To validate the feasibility of proposed scheme, results were compared with existing systems and its performance was evaluated by the detection of novel attacks while obtaining an accuracy of 94.50%.**

***Index Terms*—Intrusion Detection, Machine Learning, Neural Networks, NSL-KDD, Internet of Things Security**

I. Introduction

DUE to rapid growth of cyber technologies the proliferation of information is now easier than ever. Even though this decade has seen a massive research interest in computer systems security but the threats caused by on-line attacks are yet to be mitigated [1]. Many of the open source software are easily available due to which the expertise required to execute cyber-attacks is significantly decreased. Also, firewalls are commonly used to block malicious traffic from probing into the network but due to their high restrictive policies, they may block useful traffic thus giving high false positive rates. Apart from that, hackers still use open ports from HTTP or SMTP to gain access to the network [2]. Such events have made the availability of scalable Intrusion Detection System (IDS) a critical task.

Efficient IDS play a vital role for the protection and prevention of attacks from any anomalous activity. The main purpose of any IDS is to identify abnormal traffic patterns from normal traffic [3] [4]. Based upon functionalities, intrusion detection systems are mainly categorised as signature based intrusion detection system (SIDS) and anomaly based intrusion detection system (AIDS) [1]. In signature based systems, which are also conceived as misuse-based intrusion detection systems,the patterns are predefined in the form of signatures within the analysed data. On the contrary, anomaly based intrusion detection systems tend to assimilate the normal behaviour based on learning about system. Upon deviation from normal traffic behaviour, an alarm is generated to categorise the traffic as abnormal.

Signature based intrusion detection systems are very effective in detecting well known intrusion attempts but they fail to detect novel or variants of old attacks due to predefined signatures [3]. Next generation intrusion detection systems are based upon anomaly detection due to its vast benefits as it can detect unseen and novel attacks from streams of data. In spite of the benefits, large false-positive rate are often recorded in AIDS. Due to its capability in identifying unknown attacks, AIDS takes precedence over signature based intrusion detection.

Many approaches have been proposed to implement anomaly based intrusion detection systems but currently machine learning (ML) is a popular choice among researchers across the globe. Using ML, a variety of research efforts resulted in remarkable achievements in the area of speech recognition [5] [6] and image recognition [7] [8]. Likewise, it is also an accepted fact that the advancements in machine learning have started a new era for artificial intelligence as well as paved the way for the development of intelligent intrusion detection systems [3] [9] .

Although, the detection of anomalous patterns from a given data seems straight forward but there are several challenges which make this task difficult to achieve, such as:

1) The lack of standard anomaly detection methods. It is very difficult to use the same technique in all type of networks, because an intrusion detection method designed for a wired network might work differently in wireless networks.
2) The unavailability of real-world labelled datasets for intrusion detection systems.
3) The segregation of data from noise is also difficult as most of the classifiers would tend to adopt noise as an intrusion in network.

Different approaches have been proposed in research related to classification based solution for detection of anomalies in network. In [10], the authors proposed K-Nearest Neighbour (KNN) classification algorithm in wireless sensor networks for intrusion detection. Error rate and parameter selection for IDS is studied which separates abnormal nodes from normal nodes by observing unusual behaviours. The authors concluded that flooding attack can seriously affect the traffic flow but KNN based IDS has successfully minimized this threat. Results show that the proposed system offered high detection accuracy and speed in mitigation of attacks in WSNs.

In [11], the authors have used Random Forest (RF) algorithm for the classification of attack traffic from normal. NSL-KDD was used as benchmark dataset using 10

fold validation for classification in Waikato Environment for Knowledge Analysis (WEKA). Empirical results show that the proposed IDS has low false alarm rates and high accuracy for attacks which includes Denial-of-Service (DoS), Remote-to-Local (R2L), User-to-Root (U2R) and Probe. But this technique is more dependent upon feature reduction for its efficiency. In [1], the authors have presented an overview of restricted- Boltzmann machine, deep neural networks and recurrent neural networks based deep learning techniques. A fully connected node model (FCN) is introduced and experiments are conducted. Authors conclude that, as compared to the other established machine learning techniques such as Random Forest (RF) and Support Vector Machine (SVM), the proposed FCN model has produced high promising results for NSL-KDD dataset. However, training using hyper-parameter configurations and change in units may result in higher false positive rates. In [12], the authors have proposed a deep learning based Recurrent Neural Network approach for IDS which is trained using NSL-KDD dataset. Authors have compared the technique with many of the traditional classification approaches such as Random Forest (RF), Naive Bayesian (NB), J48 and found that Recurrent neural network based IDS has high accuracy in both 2-class and 5-class traffic in NSL-KDD dataset. But the training time was recorded high due to the feedback nature of recurrent neural networks which can be a major hurdle in the implementation of scalable IDS.

In [4], the authors have presented Artificial Neural Network (ANN) based IDS and used NSL-KDD as dataset. The system was trained and tested for normal and attack traffic which includes DDoS, U2R, R2L and Probe attacks. The authors have mentioned that in case of U2R and R2L, the used dataset contains less number of patterns by default. Levenberg-Marquardt (LM) and quasi-Newton Back propagation algorithm (BFGS) are used for training in proposed IDS. Testing the model confirmed that proposed IDS has good anomaly detection rate for 2-class and accuracy 81.2%, which is higher than other reported models. In order to reduce the increasing computational time, Random Neural Networks (RNN) [13] have generated significant results on several platforms [14] [15] [16] [3] [17] [18]. RNN is easier to execute on hardware [19]. Authors have also compared RNN with ANN which shows that even though training time for feed-forward RNN is more than ANN but runtime calculation for RNN was phenomenally less than ANN [20].

It is evident from past research findings that by using ML platforms, we can create resilient models and anticipate improved results. We are proposing a novel Random Neural Network based Intrusion Detection System (RNN-IDS) model in this paper. Random Neural Networks are feed-forward, which means less time is required to train the layers of neurons. Different algorithms are used to further reduce the training time of RNN which can be effective because, real-world data is categorized generally as "Big Data" and having less time to train the RNN model could go a long way in the implementation of scalable and efficient IDS.
The main contributions of this research are:

- Random Neural Network model has been adopted for the development of novel anomaly based Intrusion Detection System (RNN-IDS).
- NSL-KDD benchmark dataset is used for the training and testing of neurons as it contains good quantity of both normal and attack traffic data points.
- The performance of novel IDS is critically analysed and an improved accuracy is achieved by training it with randomized input data, using variant learning rates.

Paper organization is outlined as follows: Section II describes the related work. The methodology to develop proposed IDS is outlined in Section III. Experimental and evaluation results are discussed in Section IV and Section V concludes this paper.

II. Related Work

This section covers the essential knowledge related to Random Neural Networks (RNN) and Gradient Descent Algorithm (GDA).

A. Random Neural Network Model

A novel class of artificial neural networks has been proposed by Gelenbe named as Random Neural Network (RNN) [13]. RNNs have been used extensively for pattern recognition [8], communication as well as implementations of Heating, ventilation, and air conditioning (HVAC) [16] [17] to enhance energy efficiency. However no research has been reported to analyse the effectiveness of RNN's for intrusion detection systems using NSL-KDD dataset (to the best of our knowledge).
In RNN model, neurons trigger the excitation and inhabitation states whenever any signal with positive or negative potential arrives. Upon reception of $+1$ signal, a neuron goes into excitation state, and -1 inhibits the previous state of the neuron by the same potential. Signals travel between total neurons N which are fully connected to each other, as an impulse. State of neuron n_i is represented by its potential at time t, each neuron n_i has state $K_i(t)$ which is a non-negative integer. Neuron n_i is accounted to be in excited state if $K_i(t)$ > 0 but it is in idle sate if $K_i(t)$ = 0. This means, if neuron n_i is in excited state i-e $K_i(t) > 0$ it randomly transmits an impulse signal at the rate r_i towards other neuron $n_j$with following probabilities:

- It can reach neuron n_j with probability of $p^+(i,j)$ as an excitation signal.
- It can reach neuron n_j with probability of $p^-(i,j)$ as an inhibitory signal.
- It can depart the neural network with probability of $c(i)$.

Mathematically,

$$c(i) + \sum_{j=1}^{N} p^+(i,j) + p^-(i,j) = 1, \forall i, \tag{1}$$

$$w^+(i,j) = r_i p^+ + (i,j) \geq 0, \tag{2}$$

similarly

$$w^-(i,j) = r_i p^- + (i,j) \geq 0. \tag{3}$$

Combining Eq 1,2 and 3

$$r(i) = (1 - c(i))^{-}1 \sum_{j=1}^{N} [w^{+}(i,j) + w^{-}(i,j)] \quad (4)$$

In Eq 4, $r(i)$ is the transmission rate between neurons and can be written as $r(i) = \sum_{j=1}^{N} [w^{+}(i,j) + w^{-}(i,j)]$. Whereas "w" matrices determines the weight update from neurons and always hold positive values as its the product of signal transmission rate and the probabilities.

In the proposed model, N number of neurons are connected with each other to share the information based on signals which can either be a positive or negative. At neuron (i), if the arrived signal is positive its denominated by Poison rate $\Lambda(i)$ and negative signal arrives at Poisson rate $\lambda(i)$. Hence, for each node "i" the output activation function for that neurons is defined as:

$$q(i) = \frac{\lambda^{+}(i)}{r(i) + \lambda^{-}(i)}, \quad (5)$$

where

$$\lambda^{+}(i) = \sum_{j=1}^{n} q(j) r(j) p^{+}(j,i) + \Lambda(i), \quad (6)$$

and

$$\lambda^{-}(i) = \sum_{j=1}^{n} q(j) r(j) p^{-}(j,i) + \lambda(i). \quad (7)$$

Interested reader can further understand the network operation in [13].

B. Gradient Descent Algorithm

In order to obtain the minima of a function we used a first-order iterative optimization algorithm known as Gradient Descent (GD). It has been widely accepted as a common training algorithm among researchers. Fundamentally, GD minimize the cost function. The error cost function can be denoted as:

$$E_p = \frac{1}{2} \sum_{i=1}^{n} \gamma_i (q_j^p - q_j^p)^2, \gamma_i \geq 0 \quad (8)$$

where $\gamma \in (0,1)$ shows the state of output neuron i, also q_j^p is an actual differential function and q_j^p is the anticipated output value. As, per Eq 8, in order to find the local minima and reduce the value for error cost function, let us consider the relation between neurons y an z, where weights $w^{+}(y,z)$ and $w^{-}(y,z)$ are updated as follows:

$$w_{y,z}^{+t} = w_{y,z}^{+(t-1)} - \eta \sum_{i=1}^{n} \gamma_i (q_j^p - y_j^p) [\frac{\partial q_i}{\partial w_{y,z}^{+}}]^{t-1}, \quad (9)$$

similarly:

$$w_{y,z}^{-t} = w_{y,z}^{-(t-1)} - \eta \sum_{i=1}^{n} \gamma_i (q_j^p - y_j^p) [\frac{\partial q_i}{\partial w_{y,z}^{-}}]^{t-1}. \quad (10)$$

The proposed RNN-IDS model has been trained using GD. The calculated weights and biases are updated to the neurons as algorithm computes the error. Interested reader can learn more details about algorithm in [15].

III. Methodology

The proposed RNN architecture consists of the variant numbers of input, hidden and output layer neurons. It contains one-way flow of information where signals from input layers is passed on to the hidden layer. The hidden layer transforms the input according to the weight and bias it learned and passes it towards the output layer. The output layer is responsible for transforming the values it learned from the hidden layer to the scale of feasible output. An interested reader can find more about RNN signal flows here [13]. Following steps are undertaken to develop RNN-IDS

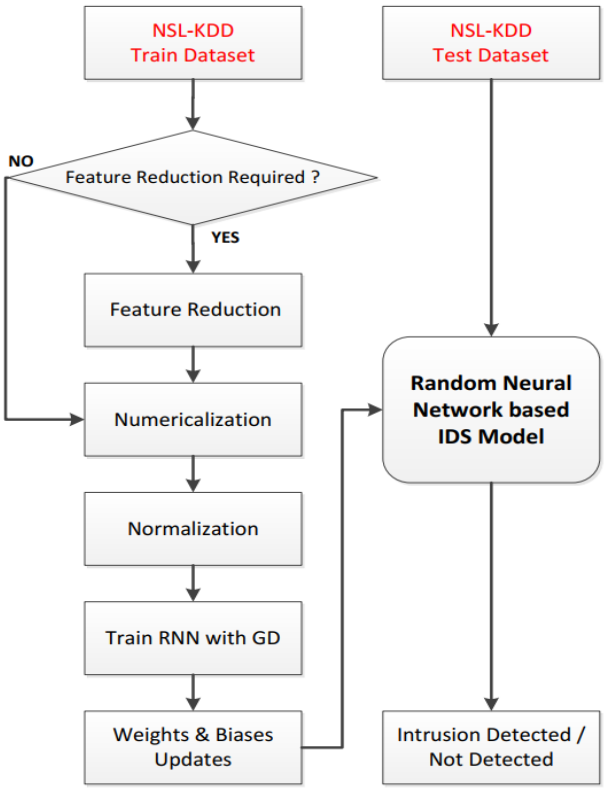

Fig. 1: Proposed RNN-IDS

system in this paper:

Data Set Selection: The proposed methodology is applied to *NSL-KDD* dataset which is a refined version of *KDDcup 99* dataset which has solved many inherent problems of benchmark [11]. Due to the removal of redundant records from KDD Cup dataset, researchers can now run complete data for training and testing purposes, but previously only a small portion was selected. Performance of classifiers has been improved due to removal of redundant and duplicate records. Although the refined dataset is not a perfect match for real-time data but due to the unavailability of real-world data for intrusion detection systems, NSL-KDD could be an effective benchmark for training and testing of network IDS against foreign attacks. Datasets types available in NSL-KDD are as shown in Table I.

The proposed scheme used *NSL-KDDTrain20* for training

TABLE I: Description of NSL-KDD Dataset [21] [1]

Dataset Type	Description	Data Points	Normal Records	Abnormal Records in %
NSL- KDD Train20	A 20% subset of NSL-KDD training data	25,192	13,499	46.6
NSL- KDD Train+	Complete NSL-KDD training data	125,973	67,343	46.5
NSL- KDD Test+	Complete NSL-KDD testing data	22,544	9711	56.9
NSL- KDD Test-	A subset of NSL-KDD testing data	11,850	2152	81.8

and *KDDTest+* for testing the model. Classification in NSL-KDD data set can be divided into binary-class and multi-class depending upon the attack traffic type [12]. Total 41 features are available in NSL-KDD dataset. The 42^{nd} feature contains output data about the different 5 classes which are categorized as one normal class and 4 attack classes. The data-points in attack class can be further categorized into Denial of Service (DoS), Probe, Remote-to-local (R2L) and User-to-Root (U2R) [1]. At this stage of research, we are only using binary-class for anomaly detection so, we have denoted Normal Records as 0 and Anomalous Records as 1.

Data Processing and Numericalization*:* Most of the attributes in NSL-KDD dataset have numeric sample data but few such as service, flag and protocol-type are non-numeric. The proposed intrusion detection model is random neural network based, so we have to convert all the non-numeric features into numeric values. This is because of the fact that input data to RNN must be a numeric matrix. Therefore, non-numeric attributes are converted into binary vectors based on their occurrence in the feature space of used dataset.

Data Normalization*:* For the efficient training of neural networks, input data should be transformed by performing some pre-processing known as data normalization. It is used where inputs are widely divergent. Without such a process, networks would take a long time to train. Different schemes can be used to normalise the input data before it is fed to the input layer of neural network. In this paper, we have used Min-Max normalization to normalize the attributes of our dataset, because of the fact that it preserves relationships between features. Value is mapped in between [0 and 1] range. Mathematically:

$$z_i = \frac{x_i - \min(x)}{\max(x) - \min(x)}, \tag{11}$$

where $x = (x_1, ..., x_n)$ is the number of input values and $z_(i)$ is the output normalized data.

Feature Reduction*:* As mentioned before, the benchmark dataset contains 41 features and 1 output class attribute. In [22], authors have applied Information Gain, Gain Ratio and Correlation based feature reduction algorithms on NSL-KDD dataset and found that some of the features such as *num_file_creations*, *num_outbound_cmds*, *dst_host_count*, *is_host_login*, *dst_host_rerror_rate*, *su_attempted* and *num_access_files* do not play significant role in detection of malicious traffic from normal patterns. More over some other features in NSL-KDD datasets have been zeroed which can also reduce the performance of IDS. In this research, we have used complete 41 features of NSL KDD data set as well as reduced features reported in [4] to validate the effectiveness of proposed RNN scheme.

IV. Experimental Results and Analysis

To evaluate the effectiveness of proposed architecture, the experiments were carried out in a controlled environment on MATLAB using Intel Core(i5) Processor with 8 GB RAM. NSL KDD dataset [21] is used to train and test RNN-IDS using Gradient Decent Algorithm (GD) for classification. Two experimental scenarios are designed.

In the first scenario, reduced features from NSL-KDD dataset reported in [4] are used with 29 input layer neurons, 21 hidden layer neurons and 1 output layer neuron for binary-class classification of attacks. In the second scenario, all 41 features of NSL-KDD data set are used. Since there is no specific formula to select best number of hidden layer neurons, the proposed scheme contains 41 input layer neurons, 41 hidden layer neurons and 1 output layer neuron for binary-class classification. Input, hidden and output layer neurons of both scenarios have been trained with variant learning rates *0.4, 0.1* and *0.01* respectively.

The efficiency of any intrusion detection system can be calculated in terms of True Positives (TP), False Positives (FP), True Negatives (TN) and False Negative (FN) respectively [3]. In the proposed RNN-IDS, whenever the intrusion is detected it is classified as TP. False classification about intrusion in the network is classified as FP. Similarly, if alert is not generated in the case where there was no real-time intrusion is categorized as TN. While FN denominates the scenario where network is intruded in real-time but RNN-IDS wrongly categorized it as non-intrusion. It can be illustrated in a confusion matrix as shown in Tab II.

The perfectness of an IDS could be defined based on its

TABLE II: Confusion Matrix

Actual	Predicted	
	Attack	Normal
Attack	TP	FN
Normal	FP	TN

efficiency to classify anomalies from normal traffic patterns. Therefore, a system which has high accuracy, low false discovery rate with good precision is categorized as an efficient system. The formulas are:

$$Accuracy\,(RNN - IDS) = \frac{TP + TN}{FP + FN + TP + TN} \tag{12}$$

$$Flase\,Discovery\,Rate = \frac{FP}{TP + FP} \tag{13}$$

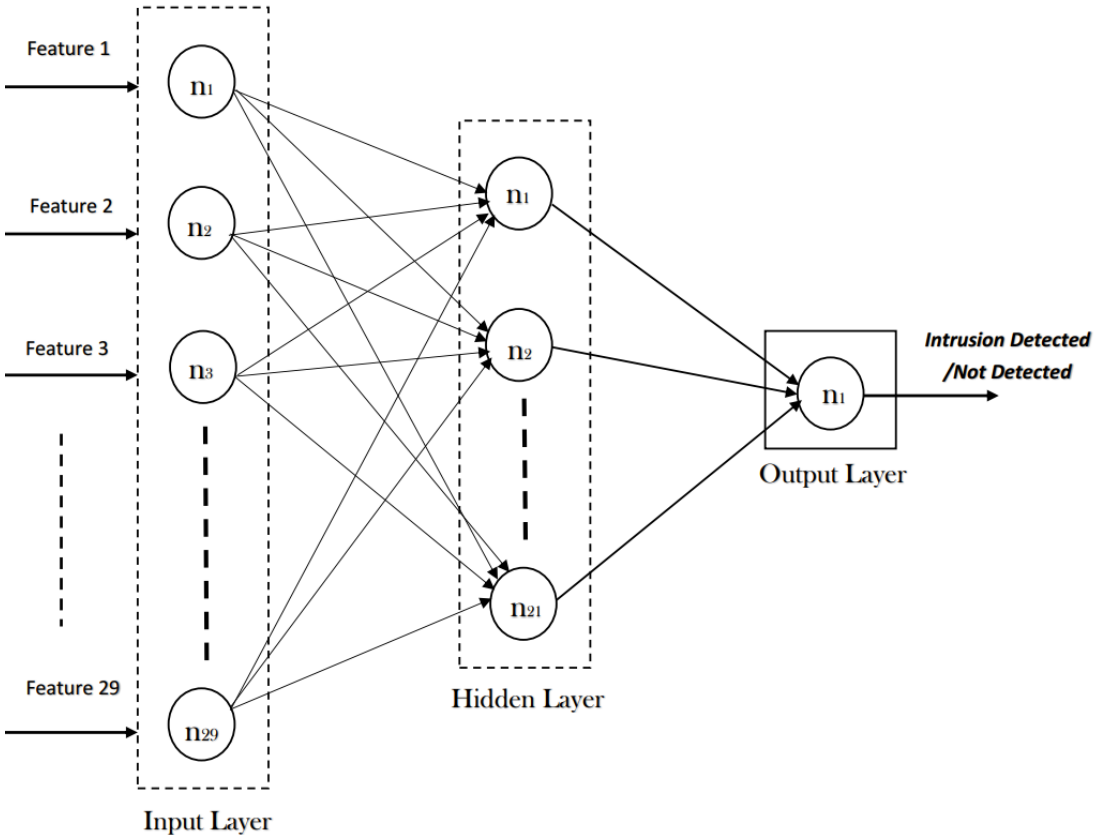

Fig. 2: System Architecture of Random Neural Network based IDS

$$Precision = \frac{TP}{TP + FP} \tag{14}$$

After training, the RNN-IDS model is tested against unseen data-points and results are collected against different performance matrices as shown in Table III and IV. The empirical results reveal that in case of 21 inputs, the accuracy for proposed RNN-IDS 91.4% which is more than reported with Artificial Neural Networks (ANN) in [4]. Low false discovery rate and higher detection rate of 94.2% is achieved with the precision of 96.6%. Similarly, in 2nd scenario where the number of input and hidden layer neurons are increased to 41×41, RNN-IDS performed even better and achieved the accuracy of 94.50%. The false discovery rate is reduced to 1% with increase in detection rate. The precision value is also increased to 98.9% as shown in Fig 3.

Based on the results shown in Table III and IV, we can derive the following facts:

- Increasing the number of input and hidden later neurons increase the efficiency of RNN-IDS
- Although learning time is high when we decrease the learning rate but in both scenarios, results proved that the RNN-IDS learned better and overall efficiency increased up to 91.4% and 94.50% respectively, when learning rate is changed to the lowest value of 0.01

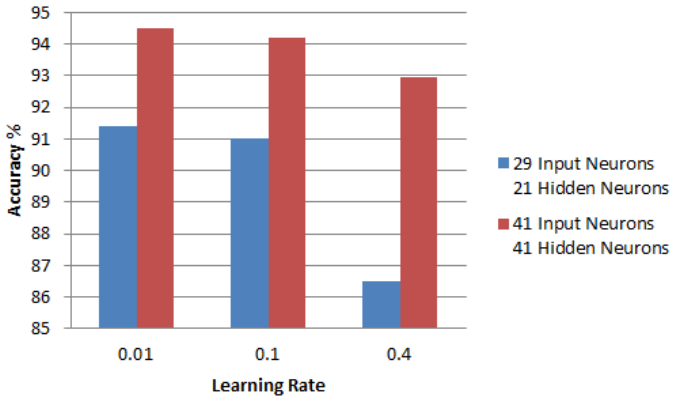

Fig. 3: Accuracy of Proposed RNN-IDS Model

- Change in learning rate also effected the Mean Square Error (MSE), as it is decreased with the decrease in learning rate.

MSE [15] can be mathematically denoted as:

$$Mean\,Square\,Error = \frac{1}{n}\sum_{i=1}^{n}(\beta_{RNN} - \beta_a)^2 \tag{15}$$

Where, β_{RNN} is the predicted intrusion based on trained RNN-IDS system while β_a is an actual intrusion.

TABLE III: Results - 29 Input and 21 Hidden Layer Neurons

Performance Metrics	Learning Rates		
	0.4	**0.1**	**0.01**
True Positive (TP)	91.72	93.36	94.24
False Negative (FN)	8.28	6.64	5.76
False Positive (FP)	6.24	2.94	3.32
True Negative (TN)	2.06	3.72	2.46
Detection Rate	91.7	93.3	94.2
Precision	93.6	96.5	96.6
False Discovery Rate	6.3	3.0	3.4
Mean Square Error	0.05	0.04	0.03
Accuracy	86.5%	91.02%	91.4%

TABLE IV: Results - 41 Input and 41 Hidden Layer Neurons

Performance Metrics	Learning Rates		
	0.4	**0.1**	**0.01**
True Positive (TP)	94.80	95.31	95.60
False Negative (FN)	5.21	5.06	4.4
False Positive (FP)	2.12	1.28	1.34
True Negative (TN)	3.13	3.44	3.08
Detection Rate	94.8	95.3	95.6
Precision	97.8	98.6	98.9
False Discovery Rate	2.1	1.3	1.0
Mean Square Error	0.04	0.04	0.03
Accuracy	92.95%	94.21%	94.50%

V. Conclusion

In this paper, we have proposed a novel Random Neural Network architecture for Intrusion Detection Systems (RNN-IDS). Feasibility of the proposed scheme is demonstrated by training an RNN Model with 41 features and reduced features with different number of hidden layer neurons using disparate learning rates. At this stage, only binary-class of NSL-KDD dataset is used for classification using Gradient Descent Algorithm (GD). The results suggest that RNN-IDS model outperformed other reported models with precision of 98.9% in detection of unknown attacks with low false positive rate while achieving the accuracy of 94.50%. It is also established that the learning rates directly effect the performance of RNN-IDS, as the mean square error is also reduced upon change in the learning rates. We would like to extend our work in future for multi-class category of NSL-KDD dataset to perform the comparative analysis with proposed Random Neural Network based IDS.

References

[1] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Computing*, pp. 1–13, sep 2017.

[2] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, jan 2016.

[3] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, "Intelligent Intrusion Detection in Low-Power IoTs," *ACM Transactions on Internet Technology*, vol. 16, no. 4, pp. 1–25, dec 2016.

[4] B. Ingre and A. Yadav, "Performance analysis of NSL-KDD dataset using ANN," in *2015 International Conference on Signal Processing and Communication Engineering Systems*. IEEE, jan 2015, pp. 92–96.

[5] A. Graves, A.-r. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, may 2013, pp. 6645–6649.

[6] G. Hinton, L. Deng, D. Yu, G. Dahl, A.-r. Mohamed, N. Jaitly, A. Senior, V. Vanhoucke, P. Nguyen, T. Sainath, and B. Kingsbury, "Deep Neural Networks for Acoustic Modeling in Speech Recognition: The Shared Views of Four Research Groups," *IEEE Signal Processing Magazine*, vol. 29, no. 6, pp. 82–97, nov 2012.

[7] J. Wan, D. Wang, S. C. H. Hoi, P. Wu, J. Zhu, Y. Zhang, and J. Li, "Deep Learning for Content-Based Image Retrieval," in *Proceedings of the ACM International Conference on Multimedia - MM '14*. New York, New York, USA: ACM Press, 2014, pp. 157–166.

[8] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," sep 2014.

[9] O. Brun, Y. Yin, E. Gelenbe, Y. M. Kadioglu, J. Augusto-Gonzalez, and M. Ramos, "Deep Learning with Dense Random Neural Networks for Detecting Attacks against IoT-connected Home Environments."

[10] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network," *Journal of Electrical and Computer Engineering*, vol. 2014, pp. 1–8, jun 2014.

[11] N. Farnaaz and M. Jabbar, "Random Forest Modeling for Network Intrusion Detection System," *Procedia Computer Science*, vol. 89, pp. 213–217, jan 2016.

[12] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21 954–21 961, 2017.

[13] E. Gelenbe, "Random Neural Networks with Negative and Positive Signals and Product Form Solution."

[14] R. Emmanuel, C. Clark, A. Ahmadinia, A. Javed, D. Gibson, and H. Larijani, "Experimental testing of a random neural network smart controller using a single zone test chamber," *IET Networks*, vol. 4, no. 6, pp. 350–358, nov 2015.

[15] J. Ahmad, H. Larijani, R. Emmanuel, M. Mannion, A. Javed, and M. Phillipson, "Energy demand prediction through novel random neural network predictor for large non-domestic buildings," in *2017 Annual IEEE International Systems Conference (SysCon)*. IEEE, apr 2017, pp. 1–6.

[16] A. Javed, H. Larijani, A. Ahmadinia, R. Emmanuel, M. Mannion, and D. Gibson, "Design and Implementation of a Cloud Enabled Random Neural Network-Based Decentralized Smart Controller With Intelligent Sensor Nodes for HVAC," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 393–403, apr 2017.

[17] A. Javed, H. Larijani, A. Ahmadinia, and D. Gibson, "Smart Random Neural Network Controller for HVAC Using Cloud Computing Technology," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 351–360, feb 2017.

[18] A. Adeel, H. Larijani, and A. Ahmadinia, "Random neural network based novel decision making framework for optimized and autonomous power control in LTE uplink system," *Physical Communication*, vol. 19, no. C, pp. 106–117, jun 2016.

[19] H. Abdelbaki, E. Gelenbe, and S. EL-Khamy, "Analog hardware implementation of the random neural network model," in *Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. IJCNN 2000. Neural Computing: New Challenges and Perspectives for the New Millennium*. IEEE, 2000, pp. 197–201 vol.4.

[20] S. Mohamed and G. Rubino, "A study of real-time packet video quality using random neural networks," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 12, no. 12, pp. 1071–1083, dec 2002.

[21] "NSL-KDD — Datasets — Research — Canadian Institute for Cybersecurity — http://www.unb.ca/cic/datasets/nsl.html, Last Accessed 2018-05-03."

[22] K. Bajaj, H. Pradesh, A. Arora, and C. University, "Improving the Intrusion Detection using Discriminative Machine Learning Approach and Improve the Time Complexity by Data Mining Feature Selection Methods," *International Journal of Computer Applications*, vol. 76, no. 1, pp. 975–8887, 2013.